CYBERWARFARE

نبرد سایبری



FirmBonyan

مؤسسه بنیان

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

جنگ سایبری

جنگ اطلاعاتی یا نبرد سایبری یك اصطلاح نسبتاً جدید است که طی سال‌های گذشته در رسانه‌ها بسیار به چشم می‌خورد؛ دستیابی به اطلاعات دشمن و استفاده از آن در جنگ، قدمتی بسیار طولانی دارد اما در عصر حاضر با شیوه‌های جدیدتری این موضوع پا به میدان نبرد گذاشته است؛ هدف از این نوع جنگ، تخریب سیستم‌های اطلاعاتی و ارتباطاتی می‌باشد؛ در واقع، با کمك این دانش، سرمایه و نیروی کار کمتری در زمینه ضربه به دشمن هزینه می‌شود.

دولت‌ها به طور فزاینده‌ای آگاه هستند که جوامع مدرن برای اجرای همه چیز از خدمات مالی گرفته تا شبکه‌های حمل و نقل آنقدر به سیستم های کامپیوتری متکی هستند که استفاده از هکرهای مسلح به ویروس یا ابزارهای دیگر برای خاموش کردن این سیستم‌ها می‌تواند به اندازه نبرد نظامی سنتی موثر و مضر باشد.



دایره و وسعت جنگ سایبری

درست مانند جنگ معمولی که می‌تواند از درگیری‌های محدود تا نبردهای تمام عیار متغیر باشد، تأثیر جنگ سایبری نیز بر اساس هدف و شدت متفاوت خواهد بود؛ در بسیاری از موارد سیستم‌های کامپیوتری هدف نهایی نیستند آنها به دلیل نقشی که در مدیریت زیرساخت‌های دنیای واقعی مانند فرودگاه ها یا شبکه‌های برق دارند مورد هدف قرار می‌گیرند؛ اگر کامپیوترها از کار بیفتند در نتیجه فرودگاه یا نیروگاه‌های برق از کار می‌افتند. در نتیجه، دولت‌ها و سازمان‌های اطلاعاتی نگران این هستند که حملات دیجیتالی علیه زیرساخت‌های حیاتی مانند سیستم‌های بانکی یا شبکه‌های برق راه را برای مهاجمان، برای دور زدن دفاع سنتی یك کشور هموار سازند.

گاها حمله سایبری پا فراتر نهاده و به منظور اهداف سیاسی، ملت را بجای دولت مورد هدف قرار می‌دهد؛ به عنوان مثال حمله به زیرساخت‌های عمرانی یك ملت می‌تواند به طور مستقیم بر افرادی که در کشور زندگی می‌کنند تأثیر بگذارد و این امر برای برانگیختن ترس استفاده شود یا باعث شود آنها در اعتراض علیه دولت شورش کنند و مخالف را از نظر سیاسی تضعیف کنند.

به نفع یك کشور است که کنترل عناصر کلیدی فضای سایبری یك کشور دشمن را به دست آورد؛ یك حمله سایبری موثر می‌تواند ارتش یك کشور دشمن را به زانو درآورد و پیروزی کم هزینه‌ای را بدست آورد.





تفاوت میان نبرد نظامی سنتی و حمله سایبری

برخلاف حملات نظامی سنتی، یک حمله سایبری را می‌توان فوراً از هر فاصله‌ای انجام داد. چنین حمله‌ای بسیار سخت است که بتوان با اطمینان عاملان آن را ردیابی کرد و انتقام‌جویی را سخت‌تر می‌کند.

اهمیت نبرد سایبری در نزد کشوری مانند روسیه

سران روسیه اهمیت ویژه‌ای برای جنگ سایبر قائل هستند؛ به گونه‌ای که در رتبه‌بندی از نظر اهمیت، جنگ سایبر را دقیقاً پس از جنگ هسته‌ای قرار می‌دهند. در سال ۱۹۹۵، یکی از فرماندهان روسی در کنفرانس مشترک روسیه - آمریکا درباره امنیت ملی در دوران پس از جنگ سرد اظهار داشت: «از دیدگاه نظامی، ما استفاده دشمنان از جنگ اطلاعاتی علیه کشور یا نیروهای مسلح روسیه را، به عنوان یک مرحله {غیرنظامی} درگیری تلقی نمی‌کنیم. با توجه به ابعاد و عواقب فاجعه‌آمیز استفاده از جنگ اطلاعاتی استراتژیک علیه نظام اقتصادی ملی و نظام فرماندهی و به‌طور کلی علیه توانمندی‌های دفاعی و رزمی روسیه، ما این حق را برای خود محفوظ می‌دانیم که در برابر ابزارها و نیروهای مهاجم اطلاعاتی و در مرحله بعد علیه خود کشور مهاجم از سلاح هسته‌ای استفاده کنیم!»



در سال‌های اخیر، چین در زمینه استفاده از فناوری نوین و نیز تغییرات فراوان در آموزش، یك انقلاب نظامی واقعی در فضای سایبر را تجربه کرده است. فعالیت‌های چین به قدری پیشرفت کرده‌است که موجب نگرانی مقامات آمریکایی شده‌است.

نتیجه

همزمان با برحذر بودن از ضربه این جنگ، مسلمانان امروزه باید برای فراگیری این دانش اهمیت ویژه‌ای قائل شوند تا بتوانند با هزینه‌های کمتر در مقابل دشمنان و اشغالگران بیشترین ضربه را به آنان وارد سازند.

